Усков А.В.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

uskov@insightbb.com
Государственный НИИ информационных технологий и телекоммуникаций
г. Москва

Вступление.

Общепризнанным стратегическим фактором роста конкурентоспособности современной образовательной организации (колледжа, университета, центра повышения квалификации и переподготовки кадров, тренинг центра, корпоративного университета, электронного университета, и т.п.) является построение и эффективное использование организацией высокоэффективной корпоративной образовательной сети (КОС).

К настоящему времени развернуто множество КОС как отдельных колледжей и/или университетов, так и малых, средних и крупных объединений колледжей или университетов. Это привело к тому, что все больше компонентов и технологий КОС, ее программных приложений и средств, электронных курсов и образовательных модулей, данных в распределенных базах данных становятся доступными большему количеству географически распределенных пользователей – в итоге, это создает значительные удобства и преимущества в их работе. Однако, обратной стороной этого процесса является тот факт, что образовательные организации сталкиваются с возрастающим числом всевозможных угроз для своих КОС – различными компьютерными вирусами, несанкционированным доступом к конфиденциальной информации, разнообразными типами компьютерных атак на инфраструктуру КОС. Так, в работе [1] приводятся данные примерно 600 респондентов – представителей больших, средних и маленьких организаций в различных областях – об обнаруженных угрозах для компьютерных сетей их организаций за последний год. Суммарное распределение обнаруженных угроз в КОС организаций-респондентов было следующим:

1. компьютерные вирусы (65% респондентов сообщили об этом типе атаки или злоупотреблении),
2. кражи корпоративных и персональных ноутбуков с конфиденциальной информацией (47%),
3. намеренное злоупотребление и/или неумышленные ошибки при работе внутри компьютерной сети (42%),
4. несанкционированный доступ к информации (32%),
5. отказ в обслуживании (25%),
6. несанкционированное проникновение в КОС (15%),
7. намеренное злоупотребление и/или неумышленные ошибки при работе в беспроводных сетях (14%),

8. кража частной конфиденциальной информации (9%),
9. финансовое мошенничество (9%),
10. телефонное мошенничество (8%),
11. ошибки в работе с открытыми Web-приложениями (6%),
12. атаки на Web-сайты (6%),
13. саботаж (3%).

В связи с этим, решение проблемы информационной безопасности (ИБ) КОС является одной из самых актуальных задач, которые стоят сегодня перед разработчиками и персоналом технического сопровождения КОС.

Технологии информационной безопасности.

Современная парадигма [2-7] обеспечения информационной безопасности компьютерной сети или системы подразумевает многоуровневую документированную программу, которая, как правило, включает активное использование:

1. на верхнем уровне: утвержденной стратегии ИБ и составляющих ее разнообразных отдельных политик ИБ,
2. на среднем уровне: обязательных базовых (международных и/или национальных) стандартов и рекомендуемых руководств,
3. на низшем уровне: отдельных технологий и средств защиты ИБ, детализированных процедур, а также многочисленных метрик защищенности системы.

Центральное место в этой цепочке занимают технологии и процедуры обеспечения ИБ. Процедуры по обеспечению ИБ описывают, как и с применением каких технологий ИБ образовательная организация должна выполнять требования, описанные в документах более высокого уровня. Следует отметить, что в настоящее время образовательные организации мира используют очень широкий спектр технологий и процедур по обеспечению ИБ КОС. В связи с этим, представляет интерес исследование эффективности применения различных технологий ИБ в КОС университетов и колледжей мира. Отборочным критерием в данном случае служила частота внедрения и/или степень активного использования технологии или процедуры ИБ в образовательных организациях в 2003-2006 годах.

Методика проведенных исследований основывалась на:

1. анализе доступных публикаций (за 2002-2007 годы) в данной области, включая около 35 доступных отчетов и публикаций по вопросам безопасности КОС больших, средних и малых образовательных организаций годах,
2. анализе выступлений и презентаций известных специалистов в области ИБ в 2002-2007 годах,
3. онланй опросе и личных интервью (проведенных в 2007 году) специалистов – системных администраторов КОС,

4. личного опыта автора по системному администрированию КОС большого (свыше 8000 пользователей) университета.

Проведенные исследований и результаты анализа многочисленных релевантных публикаций (например, [8-18])позволили сформулировать перечень наиболее часто используемых технологий и процедур обеспечения ИБ в КОС, который приведен ниже с указанием популярности по 10-бальной шкале каждой отдельной технологии или процедуры (в данном случае, 10 баллов соответствуют наилучшей технологии):

1. внешние, т.е. расположенные по периметру, брандмауеры или межсетевые экраны (МЭ) – 9.5;
2. внутренние МЭ – 9.5;
3. программное обеспечение по обнаружению и обезвреживанию компьютерных вирусов – 9.5;
4. защищенные виртуальные частные сети (VPN-сети) для удаленного доступа к КОС – 9.0; следует отметить бурный (примерно 33% в год) рост популярности внедрения и использования этой технологии за последние 2 года;
5. ограничение типов протоколов обмена данными, которым разрешается проходить через внешние и внутренние МЭ и маршрутизаторы (рутеры) КОС – 8.5;
6. существенное ограничение, а в предельном случае, даже исключение возможности (т.е. блокирование) обращения к серверам и некоторым сетевым программным системам/приложениям КОС – 8.0;
7. централизованное восстановление данных в КОС – 8.0;
8. программное обеспечение по предотвращению несанкционированной пользователем передачи от его имени данных и/или информации (anti-spyware или anti-adware) – 8.0;
9. активная фильтрация (active filtering) – 7.5 (отметим, что число организаций, внедряющих эту высокоэффективную технологию, удваивается каждый год в течение последних трех лет);
10. ограничение на продолжительность использования некоторых программных приложений КОС – 7.5;
11. контрольные листы (списки) доступа, расположенные на серверах КОС (server-based access control list) – 7.0;
12. корпоративная директория или фолдер (corporate directory) или центральный репозиторий организации – 7.0 (отметим примерно 25%-ый в год рост популярности этой технологии);
13. программные и технические средства обнаружение вторжений (intrusion detection) – 6.5;
14. технологии шифрования данных при их передаче в КОС– 6.0;
15. инфраструктура открытых ключей (PKI) – 5.5;
16. паролирование допуска в КОС и/или к отдельным ее частям и приложениям – 5.0;

17. корпоративное руководство (план, программа) по восстановлению доступности, конфиденциальности, отказоустойчивости и целостности программного и технического обеспечения и данных КОС, нарушенных в результате неправомочного (злонамеренного) использования ее ресурсов или стихийных бедствий – 4.5;
18. программные и технические средства предотвращение вторжений (intrusion prevention system) – 4.0;
19. система контроля регистраций (логинов) пользователей КОС – 4.0;
20. МЭ для отдельных программных приложений КОС (application-level firewall) – 4.0;
21. смарт-карты, одноразовые пропуска и/или другие электронные ключи для обеспечения допуска в КОС – 4.0;
22. ограничения на тип и контент, а в некоторых случаях, даже на URL конкретных Web-сайтов, которыми разрешается пользоваться в данной КОС; это достигается за счет использования технологий активной и пассивной фильтрации с помощью МЭ, и динамическим перечнем Web-сайтов, которые недопустимо использовать пользователям данной КОС) – 3.5;
23. соблюдение стандартов ИБ в КОС – 3.0;
24. программные и технические средства защиты программного обеспечения, информации и данных на отдельных пользовательских компьютерах – 3.0;
25. установка специального программного обеспечения, направленного на постоянный (24/7/365) мониторинг появления в КОС злонамеренного кода (malicious code), обнаружения случаев несанкционированного доступа, (unauthorized access), организованных атак (attacks) или вторжений (intrusion), внештатных изменений в запротоколированной и объявленной неизменности (tranquility) программных и технических средств КОС – 2.0;
26. биометрические средства аутентификации пользователей – 2.0;
27. использование специализированных физических устройств для аутентификации пользователей (например, магнитных карточек) – 1.5;
28. электронная подпись – 1.0.

Технологии безопасности беспроводных сетей.

В настоящее время в образовательных организациях наблюдается резкий рост числа аудиторий, лабораторий и пользователей, использующих беспроводной (wireless, WiFi) доступ к сетям интранет и Интернет. В связи с этим, дополнительно приведем перечень высокоэффективных технологий и процедур ИБ для КОС с беспроводным доступом; ниже указаны как показатели популярности отдельных технологий по 10-бальной шкале, так и примерный процент роста популярности данной технологии каждый год в период с 2003 по 2006 гг.:

1. WiFi МЭ – 7.0 (80%);
2. технология VPN-сетей (virtual private networks) – 7.0 (70%);
3. технология RADIUS (remote authentication dial-in user service) – 5.5 (10%);

4. технология 128-bit WEP (Wired Equivalency Privacy) – 3.5 (30%);
5. технология Kerberos – 2.0 (100%);
6. протокол EAP (Extensible Authentication Protocol) – 2.0 (200%);
7. технология 40-bit WEP (Wired Equivalency Privacy) – 2.0 (20%);
8. технологии на основе AES (Advanced encryption standard) – 1.5 (125%).

Необходимо отметить, что в настоящее время все более широкое применение находят технологии WPA (WiFi Protected Access) и WPA2. В сочетании с известными TKIP-алгоритмом и Michael-алгоритмом шифрования данных, эта технология также использует и алгоритм, основанный на использовании вышеуказанного AES стандарта и CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code) протокола. С 2006 года получение сертификата WPA2 является обязательным для всех вновь сертифицируемых WiFi устройств.

Следует особо подчеркнуть, что результаты проведенного исследования позволяют определить ярко выраженную тенденцию образовательных организаций к созданию и использованию централизованного (единого) корпоративного центра ИБ КОС (что осуществлено примерно в 62% опрошенных организациях) вместо устаревающей стратегии по использованию локальных отделов (групп) информационной безопасности образовательной сети (что на сегодня еще остается примерно в 38% организаций).

Заключение.

Ряд решений по совместному интегрированному использованию описанных выше технологий и процедур ИБ, а также предложенные методы обеспечения ИБ локальных серверов КОС были протестированы, внедрены и использованы в 2004-2007 годах в корпоративной образовательной среде достаточно большого одного университетов с более, чем 8000 физических пользователей и около 150 локальных серверов. В результате постоянного (24/7/365) мониторинга локальных серверов подразделений университета в 2004-2007 гг. было зарегистрировано а) 0 случаев успешной внешней или внутренней атаки, б) только 1 случай успешного внедрения злонамеренного кода, на защищенные локальные серверы, включая стримминг-серверы, серверы данных, Web-серверы, серверы коммуникаций. Это свидетельствует о высокой эффективности предложенных и разработанных методов защиты ИБ локальных серверов КОС.

В то же время, как указывается в [3,4,5], в результате частичного и/или фрагментарного внедрения указанных выше технологий ИБ в КОС примерно 540 колледжей и университетов США, были получены следующие обобщенные результаты по снижению в 2006 году (по сравнению с 2005 годом) уровня зарегистрированных проблем с безопасностью КОС в образовательных учреждениях [2]:

1. снижение числа организованных атак на КОС: 47% образовательных учреждений сообщили об этой проблеме в 2006 году, в то время как в 2005 году 52% организаций указывали на подобные проблемы;
2. снижение числа внедрений злонамеренного кода в (вирусов, «червей», «троянских коней», и т.п.) в КОС: 26% в 2006 году против 42% в 2005 году;
3. снижение числа проблем с аутентификацией пользователей КОС: 21% в 2006 г. против 20% в 2005 году;
4. снижение числа пропавших компьютеров (ноутбуков): 13% в 2006 году против 15% в 2005 году;
5. проблемы с пропажей информации или с несанкционированным доступом к ней на серверах, которые не были включены в демилитаризованную зону КОС: 12% в 2006 году (такие данные за 2005 год отсутствуют);
6. проблемы с некорректным или неправомочным использованием специализированных социальных Веб сайтов (social networking web sites): 10% в 2006 году (такие данные за 2005 год отсутствуют).

СПИСОК ЛИТЕРАТУРЫ

1. 2006 CSI/FBI Computer Crime and security Survey, Computer Security Institute, 2006.
2. Guide to Malware Prevention and Handling, U.S. National Institute of Standards and Technology, Washington, DC, November 2005.
3. Guide to IPsec VPNs, U.S. National Institute of Standards and Technology, Washington, DC, December 2005.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД «ФОРУМ» - ИНФРА-М, 2008.
5. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Академия АйТи, 2006.
6. Сердюк В.А. Новое в защите от взлома корпоративных систем. – М.: Техносфера, 2007.
7. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность. – М.: Издательский центр «Академия», 2005.
8. Green K. The 2006 National Survey of Information Technology in US Higher Education, The Campus Computing Project, 2006.
9. Pirani J., Voloudakis J. Information Security at Massachusets Institute of Technology, EDUCASE Center for Applied Research, 2003.
10. Adler P. A Unified Approach to Information Security Compliance, EDUCASE Review, October 2006.
11. SANS Institute: Top-20 2007 Security Risks, доступен на http://www.sans.org/top20/
12. DTI Information Security Breaches Survey 2006, доступен на http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf
13. 2006 Global Information Security Report, доступен на http://www.ey.com/global/assets.nsf/International/TSRS_-_GISS_2006/$file/EY_GISS2006.pdf

14. 2007 Global Security Survey, доступен на http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf и http://www.deloitte.com/dtt/press_release/0,1014,sid%253D1000%2526cid%253D171269,00.html
15. Global State of Information Security Survey 2007, доступен на http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B
16. Insider Threat Research, доступен на http://www.cert.org/insider_threat/
17. Anderson R., Moore T. The Economics of Information Security, доступен на http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf
18. EDUCASE: Current Issues Survey Report, 2007, доступен на http://www.educause.edu/ir/library/pdf/EQM0723.pdf

Усков А.В.

ВЫСОКОЭФФЕКТИВНЫЕ IPSEC VPN-РЕШЕНИЯ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

uskov@insightbb.com
Государственный НИИ информационных технологий и телекоммуникаций
г. Москва

Вступление.

Радикальным способом устранения уязвимостей в корпоративных образовательных сетях (КОС), основанных на использовании IP-сетей, является создание системы защиты на третьем или сетевом уровне модели OSI (таблица 1) в связи с тем, что именно сетевой уровень IP-сетей обладает наибольшей гомогенностью [1]. Поэтому, независимо от а) использования протоколов вышележащих уровней, б) физической среды передачи данных, в) конкретной технологии канального уровня, транспортировка данных по IP-сети не может быть произведена в обход IP-протокола. Размещение средств защиты на этом уровне делает их прозрачными как для сетевых приложений, так и для пользователей сети. Дополнительно, 1) на сетевом уровне существует возможность достаточно надежной реализации защиты траффика в сети управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений; 2) используемый стек протоколов IPSec обеспечивает аутентичность участников обмена данными, целостность передаваемых данных и их конфиденциальность, туннелирование трафика, шифрование IP-пакетов; 3) стек протоколов IPSec совместим как с действующей сегодня версией протокола IPv4, так и с новейшей версией IPv6, которая постепенно внедряется в сеть Интернет [2].